UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,482	12/31/2003	Jeffrey J. Jonas	SVL920050503US2	9863

22462   7590   06/11/2008
GATES & COOPER LLP
HOWARD HUGHES CENTER
6701 CENTER DRIVE WEST, SUITE 1050
LOS ANGELES, CA 90045

EXAMINER
PATEL, NIRAV B

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/750,482	JONAS, JEFFREY J.
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _07 March 2008 (RCE)_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-58_ is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-58_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _5/23/08_.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

1. Applicant's submission for RCE filed on March 07, 2008 has been entered. Claims 1-58 are

pending.

Claim Objections

2. Claims 30 and 46 are objected to because of the following informalities:

Claim 30 recites "**For a system for processing data and a computer readable storage device**

storing program instruction for...., it performs a method for processing data....", it is not clear in the

claim limitation whether it is intended to be a system claim or a computer readable storage device.

Claim 46 encompasses limitations that are similar to those of claim 30. Thus, it is objected with

the same rationale applied against claim 30 above.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section
> 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the
> subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill
> in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

3. Claims 1, 17, 21, 25, 30, 46, 50 and 54 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Voltmer et al. (US Pub. No. 2002/0112177) in view of Flink et al (US Patent No.

7,024,562) in view of Hamid (US Pub. No. 2003/0091218) and in view Epstein (US Pub. No.

2002/0124176).

As per claim 1, Voltmer teaches: an anonymous biometric authentication system and method for receiving a first biometric data and a second biometric data [Fig. 1-3, 12A, 12B, paragraph 0010, 0013]; comparing the second data to the first data and generating a signal pertaining to the comparison of the second data to the first data for use in an authentication process [paragraph 0013, 0017, 0051]. Voltmer teaches converting and/or encrypting the biometric data [paragraph 0046 lines 13-17]; discarding the credentials after the enrollment stage [paragraph 0045, 0053]. Voltmer doesn't expressively mention that processing the first biometric data combined with the first personal key.

Flink teaches: processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a first processed data; processing the second biometric data combined with the second personal key through an irreversible cryptographic algorithm to form a second processed data and comparing the second processed data to the first processed data [Fig. 3, col. 8 lines 13-31].

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Voltmer's invention according to Flink's teachings. One skilled would have been motivated to incorporate Flink's teachings because it improves the security and provides higher security level [Flink, col. 4 lines 13-22].

Voltmer and Flink don't expressively mention comparing the second processed data to the first processed data, without accessing the first and second processed data in an unprocessed form.

Hamid teaches: comparing the second processed data to the first processed data, without accessing the first and second processed data in an unprocessed form, in order to enable authentication of the first and second biometric data in a confidential manner [Fig. 9, 10, 11, paragraph 0078, 0079].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Voltmer's and Flink's invention with the teachings of Hamid, to prevent security attacks because Hamind's method that does not necessitate the storage of templates against which a fingerprint is compared [Hamid, paragraph 0020].

Hamid teaches storing the hashed enrollment value only. Hamid doesn't expressively mention eliminating all storage or trace of the unprocessed data.

Epstein teaches eliminating all storage or trace of the unprocessed data [Fig. 4, paragraph 0029].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Voltmer's, Flink's and Hamid's invention with the teachings of Epstein to provide a biometric authentication and access security method that is less susceptible to forged or copied biometric information [Epstein, paragraph 0008].

As per claim 17, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 21, the method of claim 17 wherein receiving the biometric data and the personal key occurs during an authentication process (Rejected per claim 1).

As per claim 25, the method of claim 17 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data (Rejected per claim 1).

<u>As per claim 30</u>, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

<u>As per claim 46</u>, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

<u>As per claim 50</u>, The computer readable medium for performing the method of claim 46 wherein receiving the biometric data and the personal key occurs during an authentication process. (Rejected per claim 21.)

<u>As per claim 54</u>, The computer readable medium for performing the method of claim 46 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data. (Rejected per claim 25.)

4. Claims 2-16, 18-20, 22-24, 26-29, 31-45, 47-49, 51-53, 55-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voltmer et al. (US Pub. No. 2002/0112177) in view of Flink et al (US Patent No. 7,024,562) in view of Hamid (US Pub. No. 2003/0091218) and in view Epstein (US Pub. No. 2002/0124176) and in view of Musgrave et al. (US Patent No. 6,202,151).

<u>As per claim 2</u>, the rejection of claim 1 is incorporated and Musgrave teaches: generating a first variant from the first biometric data prior to processing the first biometric data and the first personal

key through the irreversible cryptographic algorithm.   (Column 5, lines 15-19.   The Examiner is

interpreting concatenating the biometric with other data as to form a 'variant.')

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention

was made to combine Musgrave with Voltmer, Flink, Hamid and Epstein, since one would have been

motivated to provide increased security and accuracy for authentication of electronic transaction

[Musgrave, col. 3 lines 25-28].

As per claim 3, the rejection of claim 1 is incorporated and Musgrave teaches: generating a second

variant from the second biometric data prior to processing the second biometric data and the second

personal key through the irreversible cryptographic algorithm. (Column 5, lines 15-19 and Column 3,

lines 54-57.)

As per claim 4, the rejection of claim 1 is incorporated and Musgrave teaches: processing the first

biometric data through a secondary irreversible cryptographic algorithm prior to processing the first

biometric data and the second biometric data through the irreversible cryptographic algorithm.

(Column 3, lines 37-39)

As per claim 5, the rejection of claim 1 is incorporated and Musgrave teaches: adding salt to the first

biometric data and the first personal key. (Figure 3, block 28. Musgrave et al. present a 'addition data

to pad...[other] combined data,' per paragraph 15 of the applicant's specification. The Examiner is

interpreting "User Input Data" given through device 28 as 'pad data' to pad 'Combined Data' that is

biometric and public key data, as presented in both the reference and instant application.)

As per claim 6, the rejection of claim 1 is incorporated and Musgrave teaches: processing the first personal key through a cryptographic algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm. (Figure 3, blocks 32 and 34. The public key is processed with other data through the cryptographic hash algorithm 34.)

As per claim 7, the rejection of claim 1 is incorporated and Musgrave teaches: associating a first primary key to the first processed data. (Column 5, lines 45-60 and Column 6, lines 52-60. The Examiner is interpreting 'primary key' to be 'any personal inputted data' per paragraph 15 of the applicant's specification (e.g., a user inputted string). Therefore, one of the datum received in Musgrave et al., per block 28 of Figure 3, is a 'primary key.')

As per claim 8, the rejection of claim 1 is incorporated and Musgrave teaches: associating a second primary key to the second processed data. (Figure 3, block 36. Please note that the first set of data (primary key, personal key and biometric) in Musgrave et al. corresponds the second set of data in the instant application (e.g., enrollment data (all) is the "first" data in the instant application, but is called "second" in Musgrave et al.). Therefore, based on paragraph 8 of column 6, Figure 3, block 36 corresponds to both 1st and 2nd datum.)

As per claim 9, the rejection of claim 1 is incorporated and Musgrave teaches: receiving the first biometric data and the first personal key occurs during an enrollment process. (Column 6, lines 52-60.)

As per claim 10, the rejection of claim 1 is incorporated and Musgrave teaches: receiving the second biometric data and the second personal key occurs during an authentication process. (Column 3, lines 57-60.)

As per claim 11, the rejection of claim 1 is incorporated and Musgrave teaches: generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data. (Column 3, lines 49-63.)

As per claim 12, the rejection of claim 11 is incorporated and Musgrave teaches: issuing a confirmation signal allows access to a facility. (Column 6, lines 5-17.)

As per claim 13, the rejection of claim 11 is incorporated and Musgrave teaches: issuing a confirmation signal allows access to a system. (Column 6, lines 5-17.)

As per claim 14, the rejection of claim 1 is incorporated and Musgrave teaches: generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data. (Column 3, lines 49-63.)

As per claim 15, the rejection of claim 1 is incorporated and Musgrave teaches: storing the first processed data in a database. (Column 3, lines 49-63.)

As per claim 16, the rejection of claim 15 is incorporated and Musgrave teaches: the database includes a plurality of first processed data. (Column 3, lines 49-63.)

As per claim 18, the method of claim 17 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm (Rejected per claim 3).

As per claim 19, the method of claim 17 further comprising processing the biometric data through a secondary irreversible cryptographic algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm (Rejected per claim 4).

As per claim 20, the method of claim 17 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm (Rejected per claim 5).

As per claim 22, the method of claim 17 further comprising associating a primary key with the biometric data and the personal key (Rejected per claim 8).

As per claim 23, the method of claim 17 wherein the secondary data includes a secondary biometric data and a secondary personal key (Rejected per claim 1 and including the reasoning of claim 7).

As per claim 24, the method of claim 23 wherein the secondary biometric data and the secondary personal key is received during an enrollment process (Rejected per claim 23).

As per claim 26, the method of claim 25 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data (Rejected per claim 11).

As per claim 27, the method of claim 25 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data (Rejected per claim 14).

As per claim 28, the method of claim 25 wherein generating a signal allows entry into a facility when the processed data matches the secondary data (Rejected per claim 12).

As per claim 29, the method of claim 25 wherein generating a signal allows entry into a system when the processed data matches the secondary data (Rejected per claim 13).

As per claim 31 The computer readable medium for performing the method of claim 30 further comprising generating a first variant from the first biometric data prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm. (Rejected per claim 2.)

As per claim 32, The computer readable medium for performing the method of claim 30 further comprising generating a second variant from the second biometric data prior to processing the second biometric data and the second personal key through the irreversible cryptographic algorithm. (Rejected per claim 3.)

As per claim 33, The computer readable medium for performing the method of claim 30 further comprising processing the first biometric data through a secondary irreversible cryptographic algorithm prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm. (Rejected per claim 4.)

As per claim 34, The computer readable medium for performing the method of claim 30 further comprising adding salt to the first biometric data and the first personal key prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm. (Rejected per claim 5.)

As per claim 35, The computer readable medium for performing the method of claim 30 further comprising processing the first personal key through a reversible cryptographic algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm. (Rejected per claim 6.)

As per claim 36, The computer readable medium for performing the method of claim 30 further comprising associating a first primary key to the first processed data. (Rejected per claim 7.)

As per claim 37, The computer readable medium for performing the method of claim 30 further comprising associating a second primary key to the second processed data. (Rejected per claim 8.)

As per claim 38, The computer readable medium for performing the method of claim 30 wherein receiving the first biometric data and the first personal key occurs during an enrollment process. (Rejected per claim 9.)

As per claim 39, The computer readable medium for performing the method of claim 30 wherein receiving the second biometric data and the second personal key occurs during an authentication process. (Rejected per claim 10.)

As per claim 40, The computer readable medium for performing the method of claim 30 wherein generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data. (Rejected per claim 11.)

As per claim 41, The computer readable medium for performing the method of claim 40 wherein issuing a confirmation signal allows access to a facility. (Rejected per claim 12.)

As per claim 42, The computer readable medium for performing the method of claim 40 wherein issuing a confirmation signal allows access to a system. (Rejected per claim 13.)

As per claim 43, The computer readable medium for performing the method of claim 30 wherein generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data. (Rejected per claim 14.)

As per claim 44, The computer readable medium for performing the method of claim 30 further comprising storing the first processed data in a database. (Rejected per claim 15.)

As per claim 45, The computer readable medium for performing the method of claim 44 wherein the database includes a plurality of first processed data. (Rejected per claim 16.)

As per claim 47, The computer readable medium for performing the method of claim 46 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm. (Rejected per claim 18.)

As per claim 48, The computer readable medium for performing the method of claim 46 further comprising processing the biometric data through a secondary irreversible cryptographic algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm. (Rejected per claim 19.)

As per claim 49, The computer readable medium for performing the method of claim 46 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm. (Rejected per claim 20.)

As per claim 51, The computer readable medium for performing the method of claim 46 further comprising associating a primary key with the biometric data and the personal key. (Rejected per claim 22.)

As per claim 52, The computer readable medium for performing the method of claim 46 wherein the secondary data includes a secondary biometric data and a secondary personal key. (Rejected per claim 23.)

As per claim 53, The computer readable medium for performing the method of claim 52 wherein the secondary biometric data and the secondary personal key is received during an enrollment process. (Rejected per claim 24.)

As per claim 55, The computer readable medium for performing the method of claim 54 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data. (Rejected per claim 26.)

As per claim 56, The computer readable medium for performing the method of claim 54 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data. (Rejected per claim 27.)

As per claim 57, The computer readable medium for performing the method of claim 54

wherein generating a signal allows entry into a facility when the processed data matches the secondary data. (Rejected per claim 28.)

As per claim 58, The computer readable medium for performing the method of claim 54 wherein generating a signal allows entry into a system when the processed data matches the secondary data. (Rejected per claim 29.)

Response to Amendment

5.   This written action is responding to the Request for Continued Examination (RCE) dated March 7, 2008. The pending claims are rejected based on **newly found references** by Voltmer et al. (US Pub. No. 2002/0112177), Flink et al (US Patent No. 7,024,562), Hamid (US 2003/0091218) and in combination with various previously cited prior art. See new ground of rejection and therefore, the argument are moot in view of the new ground(s) of rejection.

Conclusion

6.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NP

6/4/08

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135